BIOS Update Release Notes

PRODUCTS: CD1M3128MK (Standard BIOS)

BIOS Version 0058 - MKKBLY35.86A.0058.2019.0813.1729

About This Release:

- Date: August 13, 2019
- ROM Image Checksum: 0x10F6
- ME Firmware: 11.8.60.3561
- EC Firmware: 6.6D
- Integrated Graphics
    - Option ROM: 9.0.1060
    - UEFI Driver: 9.0.1084
- AHCI Code: Based on AHCI_14
- Supported Flash Devices:

MACRONIX	MX25L6473F	8MB
WinBond	W25Q64FV	8MB
Gigadevice	GD25B64CWIGR	8MB

- Microcode Updates included in .ROM File:
  MC0806E9_000000B4.mcb
- Additional Microcode Updates included only in .BIO File:
  MC0806E9_000000B4.mcb

New Fixes/Features:

- Added Realtek PXE option ROM.
- Updated BIOS for security fixes.
- Updated BIOS code for BIOS recovery with USB flash drive.

BIOS Version 0057 - MKKBLY35.86A.0057.2019.0528.1832

About This Release:

- Date: May 28, 2019
- ROM Image Checksum: 0x2BCD
- ME Firmware: 11.8.60.3561
- EC Firmware: 6.6D
- Integrated Graphics
    - Option ROM: 9.0.1060
    - UEFI Driver: 9.0.1084
- AHCI Code: Based on AHCI_14
- Supported Flash Devices:

MACRONIX	MX25L6473F	8MB
WinBond	W25Q64FV	8MB
Gigadevice	GD25B64CWIGR	8MB

- Microcode Updates included in .ROM File:
  MC0806E9_000000B4.mcb
- Additional Microcode Updates included only in .BIO File:
  MC0806E9_000000B4.mcb

New Fixes/Features:

- Modified BIOS code for security fixes.
- Updated CPU microcode to MC0806E9_000000B4.

BIOS Version 0056 - MKKBLY35.86A.0056.2019.0315.2102

About This Release:

- Date: March 15, 2019
- ME Firmware: 11.8.60.3561
- EC Firmware: 6.6D
- Integrated Graphics
  - Option ROM: 9.0.1060
  - UEFI Driver: 9.0.1084
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Updated CPU microcode to MC0806E9_0000009A.
- Updated Intel® ME firmware to version 11.8.60.3561.
- Modified BIOS code for security fixes.
- Updated support for Windows 10 RS5.
- Updated VBIOS to version 9.0.1060.
- Updated graphics UEFI driver to version 9.0.1084.

Known Errata:

- Due to the Intel® ME firmware update in BIOS version 0056, you can't downgrade to version 0054 or earlier.

BIOS Version 0054 - MKKBLY35.86A.0054.2018.1123.1528

About This Release:

- Date: November 23, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 6.6D
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1075
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Updated setup items (F9 & CTRL-P) layout.
- Fixed UQI definition of "Event Logging" and "Allow UEFI Third Party Driver loaded".

BIOS Version 0053 - MKKBLY35.86A.0053.2018.0829.1541

About This Release:

- Date: August 29, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 6.6D
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1075
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Added BIOS setup item for Boot USB Devices First.
- BIOS code improvements for Intel® Integrator Toolkit.

BIOS Version 0052 - MKKBLY35.86A.0052.2018.0718.1614

About This Release:

- Date: July 18, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 6.6D
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1075
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Updated CPU Microcode (Security Advisory-00115).

BIOS Version 0051 - MKKBLY35.86A.0051.2018.0529.1751

About This Release:

- Date: May 29, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 6.6Dh
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1075
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Updated EC firmware to version 6.6D.
- Added security enhancements.

BIOS Version 0050 - MKKBLY35.86A.0050.2018.0327.1758

About This Release:

- Date: March 27, 2018
- ME Firmware: 11.8.50.3460
- EC Firmware: 6.6Ch
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1075
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Updated Intel® ME firmware to version 11.8.50.3460.
- Updated the GOP version.
- Updated EC firmware to version 6.6C.
- Due to a security enhancement, the BIOS cannot be downgraded to any version older than version 0050.

BIOS Version 0047 - MKKBLY35.86A.0047.2018.0227.1804

About This Release:

- Date: February 27, 2018
- ME Firmware: 11.8.50.3425
- EC Firmware: 6.6Ah
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Updated CPU Microcode (Security Advisory-00088)
- Updated EC firmware version to 6.6A.
- Fixed issue with disabling eMMC controller.
- Modified processor max speed.

BIOS Version 0044 - MKKBLY35.86A.0044.2017.1221.1834

About This Release:

- Date: December 21, 2017
- ME Firmware: 11.8.50.3425
- EC Firmware: 6.65h
- Integrated Graphics:
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Updated CPU Microcode (Security Advisory-00088)
- Fixed an issue where loading the BIOS defaults wouldn't enable "USB Boot" when it was set to disabled.
- Updated EC firmware to version 6.65h.
- Added feature to allow HDD passwords.

BIOS Version 0042 - MKKBLY35.86A.0042.2017.1108.1922

About This Release:

- Date: November 8, 2017
- ME Firmware: 11.8.50.3425
- EC Firmware: 6.5Ah
- Integrated Graphics
  - Option ROM: 9.0.1051
  - UEFI Driver: 9.0.1066
- AHCI Code: Based on AHCI_14

New Fixes/Features:

- Updated Intel® Management Engine Firmware to version 11.8.50.3425 for Security Advisory-00086.
- Updated processor support.
- Updated EC firmware to version 6.5A.
- Fixed WHCK issues: Secure Boot Manual Logo Test and WindowsToGo Boot Test.
- Added VT-d setup item.
- Fixed issue where computer cannot wake from S3/S4 via task scheduler.
- Added LAN boot support.

- Added BIOS setting for Suppress Alert Message.
- Implemented security updates.
- Updated BIOS WMI support for eject handler software.

Known Errata:
Due to a security enhancement, the BIOS version cannot be downgraded to a version earlier than BIOS 0042.

BIOS Version 0036 - MKKBLY35.86A.0036.2017.0826.0755

About This Release:

- Date: August 26, 2017
- ME Firmware: 11.7.0.3290
- EC Firmware: 6.55h
- Integrated Graphics
    - Option ROM: 9.0.1051
    - UEFI Driver: 9.0.1066

New Fixes/Features:

- Initial production BIOS release.

LEGAL INFORMATION

Information in this document is provided in connection with Intel Products and for the purpose of supporting Intel developed server/desktop boards and systems.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights. Intel products are not intended for use in medical, lifesaving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

Intel is a trademark of Intel Corporation in the US and other countries.
Copyright (c) 2017 Intel Corporation.